About QoS in DVB-S2/RCS Systems

Baptiste Jacquemin[1,2], Pascal Berthou[1,2],
Thierry Gayraud[1,2] and Lionel Bertaux[1,2]
[1]*CNRS; LAAS; 7 avenue du Colonel Roche, F-31077 Toulouse, France*
[2]*Université de Toulouse; UPS, INSA, INP, ISAE; LAAS; F-31077 Toulouse, France*

1. Introduction

The standardization of a Return Channel via Satellite and the satellite community efforts in term of interoperability over the last few years stands for major milestones in the development of reliable, efficient and low cost satellite equipments. It leads to quite a positive outcome: geostationary satellite networks are expected to play a decisive role in bridging the existing digital divide through providing broadband access to multimedia services in low terrestrial infrastructure areas.
However, unlike cable or 3GPP access networks, a lot of work on IP over satellite has been needed, especially about Quality of Service (QoS). The QoS architecture takes benefits from DVB-RCS dynamic allocation schemes and IP QoS architecture to cope with the satellite delay and the scarce uplink resources. This chapter deals with design and evaluation of Quality of Service Architecture to be implemented in DVB-S2/RCS systems.

The first section of this chapter aims at introducing DVB-S2/RCS Systems.
The long term efforts to optimize the DVB-S standard to lower the price of satellite access networks led to a new evolution of the standard: DVB-S2. A better encapsulation mechanism of IP packets and a new adaptative transmission scheme are the main concerns for the QoS architecture.
The encapsulation of IP packets in DVB-S has always been a complex problem. This section presents the evolution of the standard from the Multiprotocol Encapsulation (MPE) and the Ultra Lightweight Protocol (ULE) to the Generic Stream Encapsulation (GSE).
The Adaptive Coding and Modulation (ACM) technique that increase the network efficiency according to the weather conditions is a major evolution. The variable transmission rate impacts the QoS management and offers new perspectives for future system evolution.

DVB-S Satellite Terminals can only receive frames from the satellite. The need for a return link rapidly becomes essential so as to support emerging Internet services via satellite.
The return link access scheme in DVB-S/RCS systems is MF-TDMA. The return link is segmented into portions of time and frequency ("superframes. A Network Control Center (NCC) performs the entire satellite system control, especially Satellite Terminals synchronization and resource allocation. It periodically broadcasts a signaling frame, the TBTP (Terminal Burst Time Plan), which updates the timeslot allocation within a

superframe between every competing ST. This allocation can be dynamically modified on STs demand thanks to a bandwidth on demand protocol called Demand Assignment Multiple Access (DAMA). This system is presented here.

The next section rapidly overviews the concepts and mechanisms of Quality of Service management in basic architectures such as IETF Intserv and IETF / Diffserv. Others mechanisms such as Traffic shaping / conditioning, SLA, Scheduling and Admission control that have a main impact on the QoS are also described.

The next part aims at describing what means QoS in satellite networks thanks to the DVB-S2/RCS QoS Architecture example.
From the very first system only based on MPLS, a first architecture based on Diffserv was proposed. It was then enhanced to better fit to the DVB-RCS system in the IST project Satsix.

The next part will answer a main question related to the satellite networking systems that is: How to develop new services with Satellite Systems?
Based on our research work and results in the field, we'll explain how to use Simulation (using NS-2 or NS-3), Basic Emulation (using Linux TC/Simnet) and Advanced Emulation testbed like the one that was developed in various projects we were involved in. And we'll conclude that part with our skill on Real Deployed Systems.

The last part deals with Performance Evaluation of the described proposals. We first evaluated DVB-S/RCS NS-2 emulation model with QoS. The next way used to evaluate the proposed architecture was done through the PLATINE emulation testbed coming as the main result of the Satsix project. Our last experiment was done in the OURSES project, labeled in the Aerospace Valley research center with the following main devices from Astra (satellite), Thales Alenia Space (Gateway) and Advantech (Satellite Terminal).

To conclude this chapter, results summary and lessons learned will be given and future work will be described.

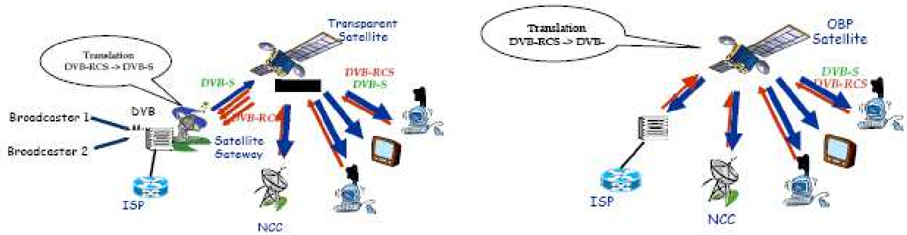
2. DVB-S2/RCS main features

2.1 First overview of DVB-S/RCS systems

Started in 1993, the international European DVB Project published, in the end-nineties, a family of digital transmission specifications, based upon MPEG-2 (Motion Picture Expert Group) video compression and transmission techniques. Data are transported within MPEG-2 transport streams (MPEG2-TS) which are identified through DVB Service Information Tables. Adapted for satellite systems, DVB-S defines one of the most widespread formats used for Digital TV over the last years and still nowadays. However, DVB-S Satellite Terminals can only receive frames from the satellite. The need for a return link rapidly becomes essential so as to support emerging Internet services via satellite, leading to 3 solutions:

- UDLR (UniDirectional Link Routing) which emulates a cheap bidirectional solution through a terrestrial return link,
- DVB-S system with low speed terrestrial return link,

– DVB-RCS, which provides a full bidirectional satellite architecture [Fig. 1].
A good overview of DVB-S/RCS satellite networks architecture is given in Fig. 1, compliant with the architecture adopted within the ETSI BSM [3] group and the DVB-RCS standards. It consists in a geostationary satellite network with Ka MF-TDMA (Multiple Frequency Time Division Multiple Access) uplinks and Ku TDM (Time Division Multiplexed) downlinks.



a) transparent satellite b) regenerative satellite
Fig. 1. DVB-S/RCS architecture

Satellite Terminals (RCST) provide single PC or LANs with the access to the network, while Gateways (GWs) allow the connection with Internet core networks. The uplink access from each RCST is managed through DVB-RCS interfaces.

On the 2 topologies, the end-user side of the platform is on the right. On the left is shown the provider/enterprise/Internet side of the platform. It can be distinguished also between the satellite network side (in the middle) and the IP network sides (on left and right ends), interconnected by RCSTs. So, the 3 main components in the satellite network side (middle) are the Satellite, the Return Channel by Satellite Terminals (RCST) and the Network Control Center (NCC).

In Fig. 1–a, the architecture relies on a transparent satellite offering a star topology. All the forward links from GW to the RCSTs are DVB-S links and all the return links are DVB-RCS links. This allows the satellite payload to work in a simple transparent way without any computation to be made on the received frames before resending. Such a payload is easier to design and was the first implemented in such GEO satellites. But the main constraints of such architecture are due to the mandatory double hop to be done to go from one RCST to another one as it is needed to go through the GW to access to an RCST.
On the opposite, this problem is solved in the second kind of architecture shown in Fig. 1–b. In this topology, the uplinks (to the satellite) are DVB-RCS links only and the downlinks (to the RCST) are DVB-S. The complexity of this solution is located in the satellite where the payload has to be regenerative to translate incoming frames in DVB-RCS in outgoing frames in DVB-S. More complex to implement, the regenerative payload was designed later than the transparent one.

It has to be noticed that it is now time to implement hybrid payload including two parts one transparent and the other one regenerative inducing more complexity of the payload, but nothing new in the architecture components where the two kinds of network components coexist, but in separated configurations.

2.2 Specific DVB-RCS features

DVB-RCS systems involve lots of specific techniques, but only a few of them impact the QoS of such a satellite network. So this section is dedicated to the 2 main ones that are DAMA and Encapsulation.

2.2.1 DVB-RCS Demand Assignment Multiple Access (DAMA)

Furthermore, DVB-RCS requires a Medium Access Control (MAC) protocol because Satellite Terminals (ST) is able to simultaneously access the return channel capacity. The standard method relies on a Multi-Frequency Time Division Multiple Access (MF-TDMA). It basically relies on the availability of several TDMA channels (corresponding to different carrier frequencies), each subdivided into frames and further into timeslots of fixed length (bursts) during which the STs are able to transmit data through MPEG2-TS or ATM traffic bursts.

The entity responsible for this timeslot allocation within the Superframe shared by competing STs is the **NCC (Network Control Center)** that centralizes the satellite resources management. Thus it periodically broadcasts a signaling frame, the TBTP (Terminal Burst Time Plan) that contains the information on which STs relies to know when to transmit their bursts. This allocation can be dynamically modified by STs requests so as to prevent from wasting satellite resources that would be otherwise statically allocated. The implementation of such a mechanism is generally known as bandwidth on demand (BoD) algorithm.

In order to dynamically manage the bandwidth allocation, a bandwidth on demand protocol called Demand Assignment Multiple Access (DAMA) is defined. It relies on the STs ability to request frequently “capacities” to the NCC which enables a regular update of the TBTP to fit to the STs respective traffic load [Fig. 2]. The latter provides signaling schemes as well as MAC QoS Classes and their mapping on capacity types.

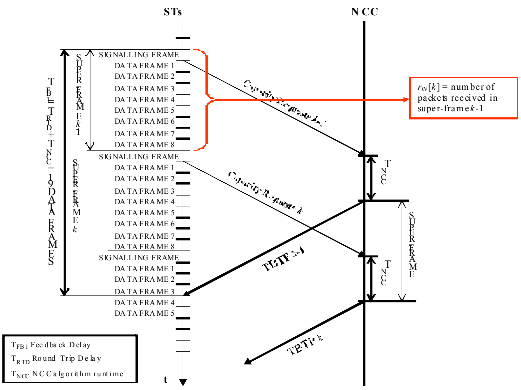


Fig. 2. DAMA algorithm: TBTP computed from RCST requests

Thus, the norm defines 5 Capacity Categories to fit the applications needs that will be detailed further in this paper. Capacity types are vital to return path QoS support at MAC layer; therefore they will be described in more details in the following. Any given ST can be

assigned one or a mix of the four capacity types. Generally, higher priority classes of service are associated with guaranteed capacity (CRA, RBDC), while lower priority classes are predominantly given best effort capacity (VBDC, FCA).
The DVB-RCS standard has left many issues open, e.g. how capacity requests are triggered, how and when certain parameters are negotiated (CRA), and if they can be re-negotiated, etc. It defines that when the NCC assigns timeslots to a certain RCST through the TBTP table, it can indicate a “channel” to which the timeslots are assigned.
It is obvious that this DAMA mechanism has great impact on what we will discuss later in this paper.

2.2.2 Encapsulation: from MPE to ULE

The multiprotocol encapsulation (MPE) provides a mechanism for transporting data networks on top of the MPEG2 TS in DVB networks. It has been adapted for carriage of IP packets, both IPv4 and IPv6. The encapsulation shall be done in accordance with the "Multiprotocol Encapsulation" technique described in the ETSI/DVB standard EN 302 192 and TR 101 202]. MPE includes methods for addressing the receivers of the data in the MPE header, which is necessary when many users have access to the same data channel. This feature allows several logical networks to be established without assigning PID values to each service.
IP datagrams are encapsulated in "datagram_sections" as defined in ISO 13818-6. The section_number and last_section _number must be "0" when carrying the IP protocol. The section format provides a format for mapping the datagram to the MPEG2 TS, and support filtering of datagram based on the MAC address using hardware or software demultiplexers.
The mapping of the datagram_section into MPEG2-TS is defined in ISO 13818-1. The sections are inserted into the payload of the MPEG2 packets (only first packet). The MPEG2 header is added to each packet. The resulting stream is the output of the data encapsulator/multiplexer, which is fed to the DVB modulator and satellite uplink equipment.
Many network operators and manufacturers of electronic equipment have adapted the MPE standard. That means that the standard is already in use and working well. Even though it is not the most efficient scheme for IP data transport.

An alternative encapsulation method has been defined by the IETF, RFC 4259. This directly places packet data into a Stream. This is called the Uni-Directional Link Encapsulation (ULE) defined in RFC 4326. The design of ULE simplifies processing, by reducing the number of header bytes and by significantly reducing the number of protocol fields that a receiver needs to parse. ULE also uses a Type field that resembles that adopted by the IEEE Ethernet standard, permitting easy interfacing to a wide range of network service (including IEEE 802.1pQ; MPLS; IPv4; IPv6).

ULE allows transmission of SNDUs up to 32 KB (compared to a maximum of 4KB in MPE). ULE also provides an extension header format (with an associated IANA registry), which allows future addition of new protocol fields to an encapsulated PDU, while providing backwards compatibility with existing implementations. This method is used to provide an efficient bridging method, but in future could also be used for encryption, compression, etc.

ULE is still old fashioned and solutions better fitted to Internet communications for instance have led to other proposal. The most promising called GSE will be presented later in this paper.

2.3 DVB-S enhancement: DVB-S2 standard and its new mechanisms

This section deals with the presentation of the new standard DVB-S2 and will be dedicated to the presentation of the main new features of such a satelite network, that are the DRA/ACM and GSE encapsulation scheme.

2.3.1 DRA/ACM

2.3.1.1 Return link

For the return link, different physical layers for individual terminals and for collective terminals have to be considered. The combination of adaptive coding, adaptive modulation and variable symbol rate can lead to different trade-offs depending on the type of scenario and of terminal.

The return link physical layer is based on the DVB-RCS standard with an adaptive waveform. DRA is considered, this means it is possible to change the coding rate, the modulation scheme and/or the transmission symbol rate. DRA is not included in the current DVB-RCS standard, but can be implemented using the standard capabilities without any additional information or changes (except for adaptive modulation using 8PSK and BPSK, which are not currently available in the DVB-RCS standard).

A DRA scheme is defined as an association of coding rate, modulation scheme and carrier symbol rate. The coding rate may be chosen among the set of DVB-RCS coding rates. Modulation can be either QPSK or 8PSK (with BPSK if required by link budgets). There is no specific constraint on the transmission symbol rate. This must be adapted to the terminal requirements in terms of the peak data rate range. However, due to equipment constraints (demodulation in particular), frequency plan constraints (in particular if the frequency plan needs to be reconfigured dynamically), the only transmitted symbol rates that are considered are multiples of each other.
A total of 70 combinations are thus possible.

The choice of DRA schemes to be retained is a trade-off between:

- the spectral efficiency (and thus the system capacity, the total number of users in the system and the average bit rate per user),
- the useful peak data rate (maximum data rate seen by a user)
- and the required SNR for each DRA scheme (the increase in required SNR should be reasonable with respect to the increase in peak rate or spectral efficiency).

When going from lowest DRA schemes to higher ones (i.e. from low SNR to a better SNR), we should:

- increase the required C/N0 with at least 2 or 3 dB steps between schemes to ensure the stability of the control loop,

- increase the spectral efficiency or the symbol peak data rate or both (that is increase the useful data rate).

When considering all possible combinations, we have 14 possible combinations of coding rate and modulation scheme, and 70 possible DRA schemes (combination of coding rate, modulation scheme and symbol rate). To select the set of DRA schemes required for the system, we consider some additional constraints resulting from implementation issues, as well as some specificity from the scenarios. We target a residential scenario with individual terminals, where we will try to optimise the spectral efficiency (to get a higher system capacity and a large number of users) rather than the peak data rate (that will be more a priority for collective terminals). However a reasonable peak data rate should still be offered to remain competitive with terrestrial solutions.
At the end, the selection process leads operational real systems to focus on around ten schemes only.

2.3.1.2 Forward link

The forward link physical layer is based on the DVB-S2 standard that supports an adaptive physical layer thanks to ACM (Adaptive Coding and Modulation). It addresses different kinds of terminals and different link conditions by allowing a large set of possible MODCOD schemes. With ACM, the coding rate and Modulation scheme can be chosen depending on the link quality within the set of available MODCOD (MODulation and CODing) schemes. The link can also be adapted dynamically by the implementation of a control loop for each station and dynamic measurement of the channel quality based on the SNIR estimation (with pilot symbols transmitted within the DVB-S2 frame).

For the forward link, there is no specific trade-off in the physical layer definition for the individual versus the collective terminals. They will all use a subset of the overall DVB-S2 possible MODCOD schemes. The MODCOD schemes retained for such systems only depend on the performances of the MODCODs proposed by the DVB-S2 standard. We select the best schemes in terms of spectral efficiency versus required Es/N0. Then the MODCODs that are actually used by individual or collective terminals will only depend on the Es/N0 range that they can reach.

This means the same DVB-S2 downlink carrier could be used to address both individual and collective terminals, the only constraint being that all the MODCOD schemes shall be supported at the same time. However, for the computations hereafter we will separate the MODCOD schemes distribution computation for individual and collective terminals.
And, as before on the return link, the selection process leads operational real systems to focus on around ten schemes only.

2.3.2 Encapsulation in DVB-S2: GSE

S2 introduces a new physical layer that supports a set of transmission waveforms that use a combination of higher-order modulation and powerful FEC coding. Although backwards-compatibility with existing DVB-S is supported, the main advantage arises when S2 is used with a range of terminal capabilities, particularly when the waveform is dynamically chosen to match the prevailing conditions of the receivers. A transmission frame consists of a 90-bit physical layer header providing a preamble and identifying the ModCod used. The payload of a physical layer frame is known as a baseband frame (BBframe) and includes a 10 byte signalling header, which is followed by the BBframe payload. The size of this payload depends on the ModCod that was selected and can be up to 8 KB, significantly larger than an MPEG-2 TS Packet. The BBframe payload may carry a sequence of TS Packets, as in other MPEG-2 networks. Therefore, PDUs can be sent by encapsulating them using MPE or ULE. In S2, the transmission is optimised by omitting any Null TS Packets from the BBframe, and re-inserting these at the Receiver (preserving end-to-end timing).

The requirements for GSE differ to those of MPEG-2 TS, in that the GS uses a strong FEC code, and a much larger frame compared to that of a TS Packet. The requirement to check the integrity of a received SNDU therefore differs from that for the MPEG-2 TS. The current proposal is not to check every SNDU, but instead to place a 32-bit CRC at the end of each BBframe. Fig. 3 shows a general picture of the different encapsulation mechanisms involved in IP communication over DVB-S2 through GSE.

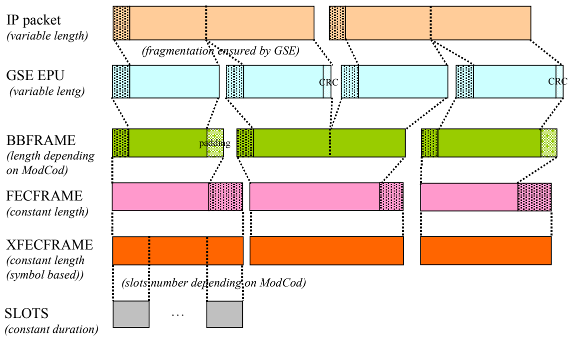


Fig. 3. GSE encapsulation in DVB-S2

The BBFRAME is the container that adapts GSE to fit the DVB-S2 properties to a data stream. DVB-S2 allows the use of a different ModCod (Modulation and Coding scheme) for each BBFRAME. This permits to take into account (while sending DVB-S2 data) the reception conditions, if available (e.g. through DVB-RCS).
A scheduling algorithm needs to take such variations into account.

In the DVB-S2 architecture, both modulation and coding can change from one BBFRAME to another, leading to variable length and variable duration BBFRAMEs. These two parameters are, however, tackled independently with the help of FECFRAMEs and XFECFRAMEs.
However, once the ModCod (more precisely the coding scheme) has been chosen, the BBFRAME length is implicitly fixed so that a padding mechanism is needed.

The FECFRAME is a constant size container that is used to encapsulate the BBFRAME with its associated coding. There are two possible values for a FECFRAME length (16200 bits or 64 800 bits) only one of which is implemented in a given system.

We will not describe more detail about FECFRAMEs, as the only pertinent information regarding a scheduler implementation is the constant length of the FECFRAME and the "variable" length of its payload.

The GSE protocol uses the BBframe header to determine the frame size (and presence of padding). The encapsulated PDUs also known as EPUs (Encapsulated Payload Units) are carried in DVB-S2 BBFRAMEs.
Not all receivers necessarily support the same set of ModCods (e.g. implementation of different sets of ModCods, different locations within the satellite footprint, local propagation conditions, or other reasons). Care therefore needs to be taken to ensure that all SNDUs or SNDU fragments are sent using GSUs with a ModCod that can be received by the intended recipient(s). Sending a SNDU or a SNDU fragment with a higher ModCod than required consumes unnecessary satellite capacity, while sending with a lower ModCod could result in loss.
At the time of writing, issues remain open such as flow security, support for signalling/control, the effect of small packets (concatenation) and these are the overall performance of the different features when used in an environment where traffic and terminal reception conditions are both varying.

3. QoS in terrestrial networks

The concept of quality of service (QoS) has gradually emerged to meet the various requirements demanded by certain types of applications, primarily in the world of interactive. Indeed, initially, the majority of Internet traffic consisted of textual data having no specific requirements but progressively, tools involving simultaneously files transfer, instant messaging, audio and video appeared. Consequently, guarantees on bandwidth, delay or jitter should be provided to users to ensure proper functioning.
However, the architecture of the Internet, based on TCP/IP, is not designed to differentiate the types of traffic and is currently dominated by a single model of service: best effort. This architecture can only guarantee correct functioning of all types of applications by offering the oversizing of the network that consists in configuring a network with a capacity that far exceeds the requirements. But this approach only postpones the problem and can hardly be applied to wireless access technologies with limited bandwidth.
Thus, effective management of resources is necessary to provide to Internet users QoS guarantees adapted to their needs. In this part, we will therefore firstly introduce the fundamentals of QoS. Then, the precursor models of QoS, IntServ and DiffServ will be detailed and finally we will show how the two signaling protocols, COPS and SIP, can participate in the implementation of QoS.

3.1 The basis of QoS

According to the standard ISO 8402 (ISO, 2000), quality of service is defined as "the totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs". The E800 recommendation ITU-T (ITU-T, 1993) defines it as "the collective effect of service performance which determines the degree of satisfaction of a user of the service".
Thus, different types of QoS can be defined from these definitions and can be separated into three categories as defined in (Hardy, 2001):

- The intrinsic quality of service that is provided directly by the network itself and described by objective parameters such as, for example, the delay or the losses. It is the primary IETF focus.
- The perceived quality of service that matches the quality perceived by the user (also called QoE, Quality of Exeprience). It depends heavily on network performance but is measured by an average of users' opinions. The most common method is the MOS (Mean Opinion Score) in which a group of users separately evaluate perceived quality of an application between 1 and 5, an average score being then performed. The MOS is typically used for audio or video quality of an application, but may also involve perceived QoS connection time, the perceived security of user, service availability, etc… In addition, there is not necessarily a correspondence between intrinsic QoS and perceived QoS, the latter being very subjective. ETSI and ITU primarily use the term QoS as perceived QoS and prefer the term network performance to describe the technical part of QoS.
- The assessed quality of service that refers to the willingness of a user to continue using a particular service. It depends on the QoS perceived but also the price, service support offered by the supplier and other commercial aspects.

The main parameters that describe the intrinsic QoS in IP networks are:

- The transfer delay of packets, in milliseconds. It is usually measured from end to end but may be calculated on a portion of the network.
- The jitter or delay variation of packet forwarding, expressed in milliseconds.
- The bit rate, expressed in bits per second (bit/s or bps) or bytes per second.
- The rate of packet loss, defined as the percentage of packets lost in relation to the total number of packets transmitted.

3.2 The main existing models to ensure QoS

Two major proposals were made by the IETF to ensure QoS and proper functioning of IP services, real time or not: IntServ (Integrated Services) and DiffServ (Differenciated Services) each associated with a working group of the same name.

3.2.1 The IntServ model

The work of the IntServ working group led in 1994 to the definition of an integrated services architecture (Braden et al., 1994) composed essentially of two parts: an extended service model, called the IS model and a reference implementation framework for the development of this model.

This architecture, allowing to support QoS without changing the IP, is based on a per flow resource reservation. Each router must maintain the state of the flows going through it, which fundamentally modifies the principle of the Internet, which, on the contrary, was till now based on a conservation of the state of flows at the user terminals. That's why routers are then equipped with four additional features:

- The packet scheduler, responsible for the delivery of packets streams, using a set of queues as well as other mechanisms such as timers.
- The classifier that realizes the correspondence between an incoming packet and the class of service to which it is associated. The level of QoS provided by each service class is programmable for each stream.

- The admission control that implements the decision algorithm used by the router to determine whether a new flow may or may not obtain the requested QoS without degrading the guarantees offered previously.
- The reservation establishment protocol, needed to create and maintain the state of flow on routers. The protocol chosen for this function is RSVP (ReSerVation Protocol), defined later as Resource reSerVation Protocol in (Braden et al., 1997).

Two new classes of service are then defined in addition to best-effort that receives no special treatment at routers:

- The Guaranteed Service (GS) (Shenker et al., 1997) provides guarantees in terms of bandwidth and maximum transfer delay of packets, expressible quantitatively. If the stream respects the reserved parameters, this service ensures that all packets will arrive with a maximum delay and that they will not be lost in the queues in case of congestion. This service is suitable for real-time applications with strong time constraints such as videoconferencing or VoIP. However, no average delay is guaranteed, so it's the application itself which has to manage the delay variations at the receiver side by using buffering mechanisms.
- The Controlled-Load service (LC) (Wroclawski, 1997) is a service expressible qualitatively in terms of bandwidth, which ensures the user that its data stream will be transmitted with a QoS close to the one obtained in a network not overloaded (not congested).

The guarantees are obtained from end-to-end by the concatenation of such assurances, offered separately by each router crossed along the path. Furthermore, as stated previously, the protocol used to configure these routers is RSVP and we will now explain its functioning.

Initially, a PATH message is propagated from the transmitter (sending application) to the receiver. This message contains the traffic specification (TSPEC) that will be generated by the application. This specification can not be modified along the path but other information can be added through additional specification (AdSpecs) to precise specific resources constraints. Once the message arrived, the receiver responds with a RESV message that contains the description of traffic flow to which the resource reservation should apply (TSPEC Receiver) and the parameters demanded to implement the required service (RSpec). These descriptions may also change along the path.

RESV messages must follow the reverse path of PATH messages and trigger an effective reservation of resources (state have to be stored at each router) if the admission control mechanisms of each router validate the request. If a router validates the request, it creates and maintains a state corresponding to this flow. However, the reservations lifespan is limited and PATH/RESV messages must be exchanged periodically so that the reservation remains valid. It allows the system to be robust to changes in routing for exemple.

Once QoS is configured, when a reserved flow is going through a router, the classifier identifies it by its 5-tuple (Source IP address, destination IP address, Protocol, TCP/UDP source port, TCP/UDP destination port). The scheduler then handles the queue management.

RSVP is so a signaling protocol that allows to reserve dynamically bandwidth and ensure a maximum delay from end-to-end. This reservation, initiated by the receiver, can prevent that some applications monopolize resources unnecessarily and allows in the case of multicast communication to differentiate the reservation (and billing) for each receiver.

Moreover, its dynamic functioning can adapt to changing communications (changes in the number of participants, route changes, etc…). Finally, this protocol also has the advantages of being adaptable to both IPv4 and IPv6 and seamlessly passing non-RSVP routers.
However, RSVP requires maintaining state information for each flow at each node or router along a path connecting a transmitter to its receiver. So, when the number of users and flows increases, the number of states becomes significant and the traffic is all the more saturated as refreshments between RSVP routers become important and create overhead. The main shortcoming of the IntServ model and the associated RSVP protocol remains their lack of adaptation to the scale factor, especially as the reservation in RSVP is unidirectional. So, for a bidirectional application requiring QoS in both directions, the amount of messages is twice as high. The IntServ/RSVP model is therefore more adapted to small networks such as LAN.
It is one of the reasons that explain that another model of architecture has been proposed: the DiffServ architecture.

3.2.2 The DiffServ model

To solve the problem of scalability posed by the per flow management of QoS in the core network routers, the DiffServ working group has therefore proposed ((Blake et al., 1998) and (Grossman, 2002)) to separate traffic by classes of service. Thus, per flow QoS treatment is realized only at edge routers that aggregate flows by traffic class. The number of state maintained by core routers is so reduced to the number of classes and not anymore to the number of flows, which greatly reduces the complexity.
Each service class is identified by a value encoded in an existing field of IP header, redefined by the DiffServ group and named DSCP (DiffServ Code Point), which presents the advantage of not requiring the use of an additional signaling protocol. This is the TOS (Type Of Service) for IPv4 and TC (Traffic Class) for IPv6.

The DiffServ architecture is primarily based on the concept of DiffServ domain that consists in the grouping of one or more networks under a single administrative authority. This domain is composed of nodes or core routers that are only connected to nodes within the same DiffServ domain and edge routers that interconnect the DiffServ domain to other domains, DiffServ or not. The edge routers can also acts as well an incoming router when the traffic enters into a DiffServ domain as an outgoing router when the traffic leaves the domain.
A client of a DiffServ domain (which can be either a user or another domain DiffServ) must negotiate a contract with the service provider responsible for this area that specifies the terms and conditions of use of the concerned services: this contract is called an SLA (Service Level Agreement) and the technical part is specified by different SLS (Service Level Specification). An SLA contains the following information:

- The traffic that the customer is likely to generate in terms of data volume, rate, number of users, etc...
- The QoS that the service provider has to provide the customer in terms of availability, security, reliability or performance (delay, bandwidth, etc…).
- The policy followed by the service provider in case of overflow traffic (rejected, accepted but surcharge, etc...).

Finally, (Nichols, 1999) defines an entity called bandwidth broker with knowledge of the resources availability and policies of the associated domain. One of its main tasks is the admission control. In addition, to allow an end-to-end allocation of resources across all the domains taking into account the different SLAs negotiated between them, this entity must communicate with the bandwidth broker of the neighbouring domains.

To manage a DiffServ domain, the service provider in charge of it first starts by sizing its network according to the contracted SLAs with all of its customers.

The processing of packets entering the DiffServ domain is then realized at the edge routers in charge of flows classification by class of service, and traffic conditioning. To do this, they are composed of a classifier, a meter, a marker, a regulator and finally a dropper of non-conforming traffic. The classifier identifies a flow from either the DSCP field only, or a combination of one or more fields such as source IP address, destination IP address, DSCP, protocol ID, source and destination ports or other information as the input interface. Then, mechanisms for profiling and traffic measurement allow on the one hand marking or re-marking the packets and, on the other hand, to shape flows or drop them totally or partially to meet the negotiated traffic profiles.

During the marking, the DSCP field is updated using one of the different classes of service or PHB (Per Hop Behaviour). In addition to the Best Effort class which is not subject to any special treatment, two PHBs have been defined by IETF:

- Expedited Forwarding (EF) (Jacobson et al., 1999) which corresponds to the highest priority and ensures the transfer of flows with high temporal constraints (eg VoIP, videoconferencing) guaranteeing a certain bandwidth and low delays, jitter and loss rate.
- Assured Forwarding (AF) (Heinanen et al., 1999) which defines four levels of priority (AF1, AF2, AF3, AF4) on the delivery of certain packets in case of congestion.

Once packets have been marked by the edge routers, they are treated within the DiffServ domain by the core routers depending on the PHB deducted from the DSCP field which describes the forwarding behavior of these routers. The priorities are then performed by scheduling algorithms such as PQ (Priority Queuing), WFQ (Weighted Fair Queuing) or CBQ (Class Based Queuing).

The DiffServ model therefore provides a QoS management more adapted and more realistic than the IntServ one. The per class management (or per aggregate) can indeed be much more resistant to the scale factor. Moreover, Diffserv does not require signaling protocol like RSVP by adapting the header of IP packets, which saves bandwidth.

However, the sizing of a DiffServ domain taking into account the SLAs contracted with neighboring domains and users is a heavy and complex task to implement that does not dynamically adapt to rapid changes in traffic. Similarly, not using a signaling protocol at the application level implies that the user is unable to dynamically change the resources according to its needs.

3.3 QoS Signaling protocol

The previous paragraphs show that, although IntServ is unsuitable for scaling up, the use of a resource reservation protocol (RSVP) allows a more precise (adapted to each stream) and dynamic QoS management. The idea of using one or more signaling protocols to negotiate and establish end-to-end QoS has consequently been the subject of a number of research among the scientific community.

The objective of this part is then to present some of these protocols that enable the implementation of QoS, the other concepts (security, supervision, etc.) being not addressed.

3.3.1 COPS and the notion of QoS management by policy

The RAP (Resource Allocation Protocol) working group of the IETF defined in 2000 an architecture based on the notion of policy to improve the admission control mechanisms of a network. A policy is defined as a set of rules for the administration, management and access control to network resources. Each rule is then associated with a set of conditions which corresponds to a series of actions to do in case of these conditions are met. To enable the exchange of such policies on a client/server model, a protocol is also defined by that working group, the protocol COPS (Common Open Policy Service) (Durham et al., 2000).

This model of by policy management is composed of two core elements: PEP (Policy Enforcement Point), responsible for implementing policy decisions and the PDP (Policy Decision Point), in charge of making decisions based on defined policy. These two components communicate via the COPS protocol. To take its decisions, the PDP communicates with a database of policies through the LDAP protocol (Leightweight Directory Access Protocol) and can query other entities such as an authentication server or a bandwidth broker using SNMP (Simple Network Management Protocol) for example.

This generic model of network control by policy allows for two distinct modes of control: outsourcing and configuration (also known as provisioning).

In the outsourcing model, a router (including PEP) which has to make a decision on acceptance of a reservation sends a COPS request to the PDP and the latter responds with the decision taken in accordance with the policy rules. It can especially be used in relation with the IntServ model when a router receives a RESV message and must decide to accept or decline the resource reservation. Indeed, that decision may require other information than the resources locally available at the router and the use of a PDP can thus be judicious.

In the configuration model, when external events require a change in the configuration of routers (and thus PEPs), the PDP may communicate to them new rules to apply through the COPS protocol. They no longer have to seek the PDP before making a decision. This model can overcome the main weakness of DiffServ model in which classes of service configuration is static. Indeed, a network administrator can define, for example, two types of policies, one appropriate to the day where many VoIP calls are held and one for the night which suits rather backup’s servers or data downloads. In this case, edge routers act as PEPs, while the bandwidth broker plays the role of PDP.

3.3.2 SIP: the session control and the QoS

SIP (Session Initiation Protocol) is a signaling protocol standardized by the IETF (Rosenberg et al., 2002) designed to establish, modify and terminate sessions with one or more participants. Its main use is now the session management of voice over IP (VoIP), for which it is currently the most common open standard, but the fact that it is independent of the type of data transmitted and the type of protocol used also allows him to develop many other applications such as instant messaging, video conferencing, distance learning, video games or virtual reality. The parameters of these sessions are described by the Session Description Protocol or SDP (Handley et al., 2006) and, in this part, we will see how these parameters can be helpful for the dynamic reservation and release of resources.

These parameters are negotiated during the establishment of the session but also during the session modifications. This negotiation can be conducted directly by the SIP clients located on users' terminals but, although they are aware of some important parameters, such as codecs they can use, the latter have no real means to know the status of available resources along the path their communications will cross. Moreover, it would imply the integration of QoS mechanisms such as RSVP or COPS on SIP clients, which has the double disadvantage of making the SIP clients more complex and not allowing SIP clients which are unaware of QoS to use this option.
That's why these new features must be rather implemented at the SIP proxy: the intermediate entities where SIP clients are registered and that intercept SIP messages. Indeed, they may allow operators to know the duration of the session, the number of involved media, the codecs used and their associated characteristics (bandwidth, etc..). From this information, automatic management of the resources reservation/release and of admission control according to the policy adopted by the operator becomes feasible and no changes are required at the SIP clients.
Two modes of session establishment with QoS reservation can then be distinguished:

- The "enabled" mode in which the session establishment and resource reservation are performed in parallel but do not depend on each other. The session will start regardless of the outcome of the reservation. For example in the case of DiffServ networks, QoS will be BE if the reservation has failed and EF if it worked.
- The "assured" mode in which the establishment of the session is done only if the QoS reservation has been realized.

A standard (Camarillo et al., 2002) detailing the operation of these two modes has been proposed. It is based on new messages such as Session Progress, UPDATE or PRACK and a set of preconditions added to the session descriptors. The SIP clients can then specify whether the implementation of QoS is "mandatory" ("assured" mode) or "optional" ("enabled" mode) for each direction of communication (reception, transmission) and if the QoS must be e2e (end-to-end) or local (at the access network). However, RFC 3312 (Camarillo et al., 2002) considers that QoS is implemented by the participants of the SIP session while we will consider that it is implemented by the SIP proxy. The Fig. 4 illustrates an example of a SIP session integrating resource reservation/release in "assured" mode.

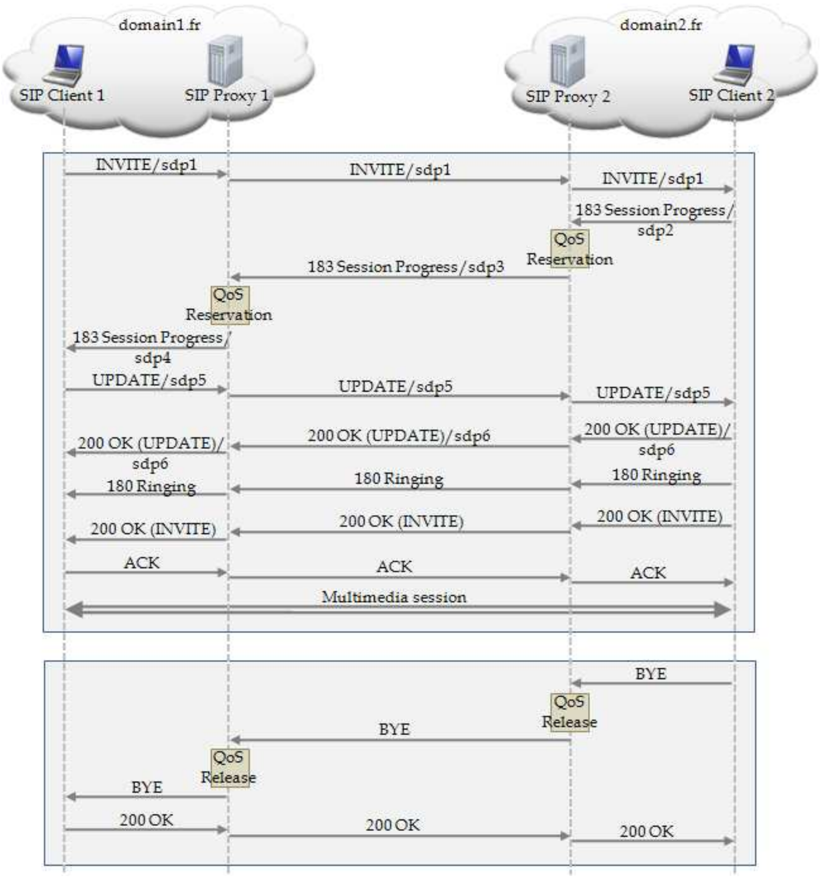


Fig. 4. SIP session with resources reservation/release

PRACK and 200 OK (PRACK) messages are not presented to make the figure more comprehensible but they are normally exchanged at the reception of a 1xx message to make it reliable. It can also be noticed that, in this example, all messages are exchanged via all the SIP proxies to manage the QoS along the whole path. Finally, QoS reservation/release in Fig. 4 may for example represent the exchange of messages (COPS, RSVP, etc..) allowing SIP proxies to communicate with the entities responsible for resources management within the concerned domains. For example, if we consider a DiffServ domain between domain1.fr and domaine.fr, the SIP proxies will be able to exchange COPS messages with the Bandwidth Broker in charge of the DiffServ domain. The latter can then configure the edge routers of this domain to prioritize the flows of the future SIP session.

Moreover, whatever the session establishment mode is, if a change of session is triggered by a re-INVITE message, SIP proxies can analyze the new parameters and automatically warn the entities responsible for resource management. The SIP signaling thus allows much more dynamic management of QoS for the applications it controls.

SIP, although it was designed originally to allow the session control, can be used very efficiently in the dynamic management of QoS.

4. QoS in satellite networks: DVB-S2/RCS QoS Architecture

The quality of service in DVB-S2/RCS networks is basically managed at layer 2. The first section gives an overview of classical layer 2 QoS architecture. The QoS offer should satisfy the application QoS requirements then this relationship is covered by the upper layers. Three QoS management strategies that can be considered as three different architecture maturity degrees are presented in this section. The first one, corresponding to a short term technique to introduce QoS in satellite system is based on MPLS over satellite systems. Then a fully IP based solution is presented as a medium term solution and the complete integration of satellite networks in Next Generation Networks (NGN) consists in the long term evolution of theses architectures.

4.1 Layer 2 QoS management

- In star architectures, the gateway (GW) centralizes the traffic and the signaling path and uses all of the offered bandwidth. Then, the quality of service management could be simply ensured by a correct scheduling algorithm, according to the packets destination and their service classes.
  But, when considering meshed topologies, the return link is shared among multiples satellite terminals. As one of the first things that impact the quality of service in the satellite network is the network access, packets should be sent on the air interface as soon as possible or even compliantly with the delay or the bandwidth required by the application. Then, in theses architectures, the quality of service management is essentially assured for the return link, i.e the DVB-RCS part.
  As said previously, the DAMA request/assignment cycle exhibits a non negligible latency and additional delays that cannot always match interactivity requirements of multimedia services. In order to both maximize satellite resource use and meet multimedia requirements, the DVB-RCS norm discriminates RCST capacity requests into 5 categories:
- Continuous Rate Assignment (CRA): Fixed slots are assigned in each MF-TDMA frame for the whole duration of a RCST connection
- Rate-Based Dynamic Capacity (RBDC): a dynamic rate capacity (in slots/frame) granted in response to explicit RCST requests
- Volume-Based Dynamic Capacity (VBDC & AVBDC): a dynamic cumulative volume capacity (in slots), granted in response to explicit RCST requests
- Free Capacity Allocation (FCA), which is assigned to STs on an “as available” basis from unused capacity

The standard defines separate MAC traffic priority queues and suggests a requesting strategy for each of them, that is to say a relevant mapping between traffic and request categories. Any given RCST can be assigned one or a mix of the four capacity types. In general, higher priority classes of service are associated with guaranteed capacity (CRA, RBDC), while lower priority classes are predominantly given best effort capacity (VBDC, FCA).

The generally recommended MAC queues are the following: